

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED	LOGGED
RECEIVED	
SEP 03 2019	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)TWO CELL PHONES, STORED AT 400 E MILL PLAIN  
BOULEVARD IN VANCOUVER, WASHINGTON

Case No.

MJ19-5167

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. 2113(b)Offense Description  
Bank Theft

The application is based on these facts:

See attached Affidavit of Special Agent Benjamin Long.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

By [Signature]  
 Applicant's signature

Benjamin Long, Special Agent (FBI)  
 Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone (specify reliable electronic means).

Date: September 3, 2019

[Signature]  
 Judge's signature

City and state: Tacoma, Washington

Hon. Theresa L. Fricke, United States Magistrate Judge  
 Printed name and title

**AFFIDAVIT**

STATE OF WASHINGTON     )  
  )  
COUNTY OF PIERCE     )     ss

I, BENJAMIN LONG, being duly sworn under oath, depose and say:

**AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigations ("FBI") and have been so employed since 2012. I am currently assigned to the Vancouver, Washington Resident Agency of the Seattle, Washington Division. Prior to serving as a Special Agent, I was employed as a law enforcement officer since 2007.

2. While employed by the FBI, I have investigated federal criminal violations related to cyber-crime, child exploitation, terrorism, civil rights violations, extortion and fraud. I have received investigative training and gained experience through the FBI Academy, Digital Evidence Extraction Technician forensic training, and the usual course of work conducting the aforementioned types of investigations. I have participated in the execution of numerous arrest and search warrants, which have resulted in arrests, convictions and the recovery of evidence and contraband.

3. The facts set forth in this Affidavit are based on my personal knowledge; knowledge obtained from others during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to

1 believe that evidence, fruits, and instrumentalities of bank theft, in violation of 18 U.S.C.  
2 § 2113(b) will be found on the SUBJECT PHONES.

3 **PURPOSE OF AFFIDAVIT**

4 5. I make this affidavit in support of an application under Rule 41 of the  
5 Federal Rules of Criminal Procedure for a search warrant authorizing the examination of  
6 property—electronic devices, namely cell phones—which are currently in law  
7 enforcement possession, and the extraction from that property of electronically stored  
8 information described in Attachment B to this Affidavit.

9 6. The property to be searched are the following two phones (collectively, the  
10 “SUBJECT PHONES”), currently in the custody of the FBI, located at 400 E. Mill Plain  
11 Boulevard in Vancouver, Washington:

12 a. A Samsung Galaxy J7 Prime, Model Number SM-G610M/DS,  
13 Serial Number R58J92RGDSW (hereinafter described as “SUBJECT PHONE 1”).

14 b. An iPhone 7, Model A1661, IMEI 355840088773379 (hereinafter  
15 described as “SUBJECT PHONE 2”).

16 7. The applied-for warrant would authorize the forensic examination of the  
17 SUBJECT PHONES for the purpose of identifying electronically stored data, particularly  
18 described in Attachment B.

19 8. Based on my training and experience, and the facts set forth in this  
20 affidavit, there is probable cause to believe that owners of these phones, PEDRO LEON  
21 RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, and JOSSHOA  
22 PEREZ RIVAS, have committed violations of Title 18, United States Code, Section  
23 2113(b) (Bank Theft). There is also probable cause to search the SUBJECT PHONES  
24 for evidence, instrumentalities, or fruits of these crimes, further described in Attachment  
25 B.

26 9. This affidavit is to be presented electronically pursuant to Local Criminal  
27 Rule CrR 41(d)(3).  
28

**PROBABLE CAUSE****A. Jackpotting Offenses**

10. On February 25, 2018, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, and JOSSHOA PEREZ RIVAS were arrested in the District of Utah while they, along with others, were "jackpotting" an ATM owned by Deseret First Credit Union in Sandy, Utah. In jackpotting attacks, perpetrators install malware, causing ATMs to dispense their cash reserves upon command. At the time of their arrest, the Deseret First Credit Union ATM was dispensing large quantities of cash, ultimately amounting to \$38,800.

11. On March 7, 2018, RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS were indicted for Conspiracy to Commit Computer Fraud and Abuse, in violation of 18 U.S.C. § 1030, Conspiracy to Commit Bank Theft, in violation of 18 U.S.C. § 371, and Bank Theft, in violation of 18 U.S.C. § 2113(b).

12. In addition to the Utah offenses, RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS also jackpotted ATMs in the Western District of Washington. As a result, on April 4, 2018, RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS were indicted in the Western District of Washington, charged with Conspiracy to Commit Bank Theft, in violation of 18 U.S.C. § 371, and Bank Theft, in violation of 18 U.S.C. § 2113(b). As alleged in that indictment, RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS jackpotted ATMs on or about the following dates:

<b>Date</b>	<b>Description</b>
12/13/17	At least \$88,000 stolen from a Sound Credit Union ATM located in Bothell, Washington by jackpotting.
12/15/17	At least \$102,400 stolen from an IQ Credit Union ATM located in Vancouver, Washington by jackpotting.
12/16/17	At least \$16,000 stolen from an Umpqua Bank ATM in Vancouver, Washington by jackpotting.
12/16/17	At least \$91,000 stolen from a Columbia Credit Union ATM in Vancouver, Washington by jackpotting.

Date	Description
12/17/17	At least \$64,400 stolen from a Heritage Bank ATM in Mount Vernon, Washington by jackpotting.

13. On December 4, 2018, January 30, 2019, and March 1, 2019, respectively, PEREZ RIVAS, GARCIA CARABALLO, and RIVERO VELAZQUEZ each pled guilty to Conspiracy to Commit Bank Theft, in violation of 18 U.S.C. § 371, in the District of Utah. In the statements of fact supporting each of their pleas, PEREZ RIVAS, GARCIA CARABALLO, and RIVERO VELAZQUEZ admitted that they jackpotted ATMs in both Utah and Washington. Although the Utah guilty pleas resolved the Washington charges against GARCIA CARABALLO and RIVERO VELAZQUEZ, PEREZ RIVAS still faces additional charges in the Western District of Washington.

**B. Seizure of the SUBJECT PHONES**

14. On February 25, 2018, after RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS were arrested in Utah, law enforcement seized the SUBJECT PHONES. RIVERO VELAZQUEZ, GARCIA CARABALLO, and PEREZ RIVAS have been in custody since the date of their arrests.

15. Agents seized SUBJECT PHONE 1 from a Nissan Rogue that RIVERO VELAZQUEZ was driving during the jackpotting attack. Law enforcement retrieved SUBJECT PHONE 1 from the driver's seat of the Rogue, after obtaining a warrant to search this vehicle. Stored in between SUBJECT PHONE 1 and its phone case, law enforcement located a photocopy of RIVERO VELAZQUEZ's identification card.

16. Agents seized SUBJECT PHONE 2 from a GMC Acadia that GARCIA CARABALLO was driving during the jackpotting attack. PEREZ RIVAS was a passenger in this vehicle. Law enforcement retrieved SUBJECT PHONE 2 from the front passenger's seat of the Acadia, after obtaining a warrant to search this vehicle.

17. Both of the SUBJECT PHONES are password protected and the contents of these phones have not been reviewed by law enforcement. The SUBJECT PHONES are currently in storage at 400 E Mill Plain Boulevard in Vancouver, Washington. In my

1 training and experience, I know that SUBJECT PHONES have been stored in a manner  
2 in which their contents are, to the extent material to this investigation, in substantially the  
3 same state as they were when the SUBJECT PHONES first came into the possession of  
4 the FBI.

5 **C. Proffer Interviews**

6 18. After their arrests, PEREZ RIVAS, GARCIA CARABALLO, and  
7 RIVERO VELAZQUEZ were each interviewed by law enforcement, pursuant to proffer  
8 agreements. During the proffer interviews, GARCIA CARABALLO and PEREZ RIVAS  
9 agreed to allow law enforcement to search SUBJECT PHONE 2, and RIVERO  
10 VELAZQUEZ agreed to allow law enforcement to search SUBJECT PHONE 1.  
11 Accordingly, while law enforcement might already have all necessary authority to  
12 examine the SUBJECT PHONES, I seek this additional warrant out of an abundance of  
13 caution to be certain that an examination of the SUBJECT PHONES will comply with the  
14 Fourth Amendment and other applicable laws.

15 19. During the proffer interviews, none of these individuals were able to recall  
16 the passwords needed to access the SUBJECT PHONES. Additionally, all explained that  
17 they only possessed these phones for a short time duration, purchasing them upon their  
18 arrival in Utah to use as “burner phones.” And many of the purchased phones were the  
19 same color, manufacturer, and model. Accordingly, while PEREZ RIVAS, GARCIA  
20 CARABALLO, and RIVERO VELAZQUEZ appear to be the most likely owners of  
21 these devices—since law enforcement retrieved the SUBJECT PHONES from vehicles  
22 PEREZ RIVAS, GARCIA CARABALLO, and RIVERO VELAZQUEZ were driving—  
23 out of an abundance of caution, law enforcement seeks further authorization to search the  
24 SUBJECT PHONES pursuant to a warrant.

25 20. At their proffer interviews, PEREZ RIVAS, GARCIA CARABALLO, and  
26 RIVERO VELAZQUEZ explained that, during the jackpotting attacks, they  
27 communicated with each other using the SUBJECT PHONES. For example, according  
28 to RIVERO VELAZQUEZ, while PEREZ RIVAS installed malware on the ATMs,

1 GARCIA CARABALLO, RIVERO VELAZQUEZ, and PEREZ RIVAS each dialed into  
2 a conference call line using their cellphones. By maintaining this conference call,  
3 GARCIA CARABALLO and RIVERO VELAZQUEZ could alert PEREZ RIVAS to  
4 police presence. In this conference call, PEREZ RIVAS also received instructions from  
5 another individual, believed to be located in Mexico, who provided PEREZ RIVAS with  
6 instructions on how to gain access to the ATM and to install the malware.

7 21. In addition to dialing into a conference call line, PEREZ RIVAS, GARCIA  
8 CARABALLO, and RIVERO VELAZQUEZ also used cellphones to exchange text  
9 messages to organize and carry out the jackpotting attacks. For example, according to  
10 GARCIA CARABALLO, he communicated with PEREZ RIVAS and RIVERO  
11 VELAZQUEZ using the encrypted chat application, WhatsApp, while in Utah. Upon  
12 arriving in Utah, each joined a WhatsApp group chat to discuss their plans to jackpot  
13 ATMs, including coordinating their travel and jackpotting targets.

14 22. Law enforcement has reviewed the contents of another cellphone, seized  
15 from JOAO SILVA ROBERTSON—one of the individuals who joined PEREZ RIVAS,  
16 GARCIA CARABALLO, and RIVERO VELAZQUEZ jackpotting ATMs in Utah and  
17 Washington—pursuant to his consent. Law enforcement located communications in this  
18 phone, which are consistent with the text messages described by GARCIA  
19 CARABALLO. For example, on February 25, 2018, SILVA ROBERTSON received a  
20 text message from PEREZ RIVAS, referencing a park located near one of the banks that  
21 PEREZ RIVAS, GARCIA CARABALLO, and RIVERO VELAZQUEZ jackpotted in  
22 Utah. On that same date, SILVA ROBERTSON placed and received numerous calls  
23 from PEREZ RIVAS, GARCIA CARABALLO, and RIVERO VELAZQUEZ. All were  
24 arrested in Utah later that day, on February 25, 2018.

#### 25 **TECHNICAL TERMS**

26 23. Based on my training and experience, I use the following technical terms to  
27 convey the following meanings:  
28



1           a.     Wireless telephone: A wireless telephone (or mobile telephone, or  
2 cellular telephone, or cellphone) is a handheld wireless device used for voice and data  
3 communication through radio signals. These telephones send signals through networks  
4 of transmitter/receivers, enabling communication with other wireless telephones or  
5 traditional "land line" telephones. A wireless telephone usually contains a "call log,"  
6 which records the telephone number, date, and time of calls made to and from the phone.  
7 In addition to enabling voice communications, wireless telephones offer a broad range of  
8 capabilities. These capabilities include: storing names and phone numbers in electronic  
9 "address books;" sending, receiving, and storing text messages and e-mail; taking,  
10 sending, receiving, and storing still photographs and moving video; storing and playing  
11 back audio files; storing dates, appointments, and other information on personal  
12 calendars; and accessing and downloading information from the Internet. Wireless  
13 telephones may also include global positioning system ("GPS") technology for  
14 determining the location of the device.

15           b.     Digital camera: A digital camera is a camera that records pictures as  
16 digital picture files, rather than by using photographic film. Digital cameras use a variety  
17 of fixed and removable storage media to store their recorded images. Images can usually  
18 be retrieved by connecting the camera to a computer or by connecting the removable  
19 storage medium to a separate reader. Removable storage media include various types of  
20 flash memory cards or miniature hard drives. Most digital cameras also include a screen  
21 for viewing the stored images. This storage media can contain any digital data, including  
22 data unrelated to photographs or videos.

23           c.     Portable media player: A portable media player (or "MP3 Player" or  
24 iPod) is a handheld digital storage device designed primarily to store and play audio,  
25 video, or photographic files. However, a portable media player can also store other  
26 digital data. Some portable media players can use removable storage media. Removable  
27 storage media include various types of flash memory cards or miniature hard drives. This  
28 removable storage media can also store any digital data. Depending on the model, a



1 portable media player may have the ability to store very large amounts of electronic data  
2 and may offer additional features such as a calendar, contact list, clock, or games.

3 d. GPS: A GPS navigation device uses the Global Positioning System  
4 to display its current location. It often contains records of the locations where it has been.  
5 Some GPS navigation devices can give a user driving or walking directions to another  
6 location. These devices can contain records of the addresses or locations involved in  
7 such navigation. The Global Positioning System (generally abbreviated "GPS") consists  
8 of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely  
9 accurate clock. Each satellite repeatedly transmits by radio a mathematical representation  
10 of the current time, combined with a special sequence of numbers. These signals are sent  
11 by radio, using specifications that are publicly available. A GPS antenna on Earth can  
12 receive those signals. When a GPS antenna receives signals from at least four satellites, a  
13 computer connected to that antenna can mathematically calculate the antenna's latitude,  
14 longitude, and sometimes altitude with a high level of precision.

15 e. PDA: A personal digital assistant, or PDA, is a handheld electronic  
16 device used for storing data (such as names, addresses, appointments or notes) and  
17 utilizing computer programs. Some PDAs also function as wireless communication  
18 devices and are used to access the Internet and send and receive e-mail. PDAs usually  
19 include a memory card or other removable storage media for storing data and a keyboard  
20 and/or touch screen for entering data. Removable storage media include various types of  
21 flash memory cards or miniature hard drives. This removable storage media can store  
22 any digital data. Most PDAs run computer software, giving them many of the same  
23 capabilities as personal computers. For example, PDA users can work with word-  
24 processing documents, spreadsheets, and presentations. PDAs may also include global  
25 positioning system ("GPS") technology for determining the location of the device.

26 f. IP Address: An Internet Protocol address (or simply "IP address") is  
27 a unique numeric address used by computers on the Internet. An IP address is a series of  
28 four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every

1 computer attached to the Internet computer must be assigned an IP address so that  
2 Internet traffic sent from and directed to that computer may be directed properly from its  
3 source to its destination. Most Internet service providers control a range of IP addresses.  
4 Some computers have static—that is, long-term—IP addresses, while other computers  
5 have dynamic—that is, frequently changed—IP addresses.

6 g. Internet: The Internet is a global network of computers and other  
7 electronic devices that communicate with each other. Due to the structure of the Internet,  
8 connections between devices on the Internet often cross state and international borders,  
9 even when the devices communicating with each other are in the same state.

10 24. Based on my training, experience, and research, and from consulting the  
11 manufacturer's advertisements and product technical specifications available online at  
12 <http://www.apple.com/iphone> and <https://www.samsung.com/global/galaxy>, I know that  
13 the SUBJECT PHONES have capabilities that allow them to serve as a wireless  
14 telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.  
15 In my training and experience, examining data stored on devices of these types can  
16 uncover, among other things, evidence that reveals or suggests who possessed or used the  
17 device.

#### 18 **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

19 25. Based on my knowledge, training, and experience, I know that electronic  
20 devices can store information for long periods of time. Similarly, things that have been  
21 viewed via the Internet are typically stored for some period of time on the device. This  
22 information can sometimes be recovered with forensic tools.

23 26. *Forensic evidence.* As further described in Attachment B, this application  
24 seeks permission to locate not only electronically stored information that might serve as  
25 direct evidence of the crimes described on the warrant, but also for forensic electronic  
26 evidence that establishes how the SUBJECT PHONES were used, the purpose of their  
27 use, who used them, and when. There is probable cause to believe that this forensic  
28 electronic evidence might be on the SUBJECT PHONES because:

1           a.     Data on the storage medium can provide evidence of a file that was  
2 once on the storage medium but has since been deleted or edited, or of a deleted portion  
3 of a file (such as a paragraph that has been deleted from a word processing file).

4           b.     As explained herein, information stored within a computer and other  
5 electronic storage media may provide crucial evidence of the “who, what, why, when,  
6 where, and how” of the criminal conduct under investigation, thus enabling the United  
7 States to establish and prove each element or alternatively, to exclude the innocent from  
8 further suspicion. In my training and experience, information stored within a computer  
9 or storage media (e.g., registry information, communications, images and movies,  
10 transactional information, records of session times and durations, internet history, and  
11 anti-virus, spyware, and malware detection programs) can indicate who has used or  
12 controlled the computer or storage media. This “user attribution” evidence is analogous  
13 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
14 The existence or absence of anti-virus, spyware, and malware detection programs may  
15 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
16 computer owner and/or others with direct physical access to the computer. Further,  
17 computer and storage media activity can indicate how and when the computer or storage  
18 media was accessed or used. For example, as described herein, computers typically  
19 contain information that log: computer user account session times and durations,  
20 computer activity associated with user accounts, electronic storage media that connected  
21 with the computer, and the IP addresses through which the computer accessed networks  
22 and the internet. Such information allows investigators to understand the chronological  
23 context of computer or electronic storage media access, use, and events relating to the  
24 crime under investigation.<sup>1</sup> Additionally, some information stored within a computer or  
25

26  
27 <sup>1</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the  
28 computer used an internet browser to log into a bank account in the name of John Doe; b) at  
11:02am the internet browser was used to download child pornography; and c) at 11:05 am the

1 electronic storage media may provide crucial evidence relating to the physical location of  
2 other evidence and the suspect. For example, images stored on a computer may both  
3 show a particular location and have geolocation information incorporated into its file  
4 data. Such file data typically also contains information indicating when the file or image  
5 was created. The existence of such image files, along with external device connection  
6 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
7 camera or cellular phone with an incorporated camera). The geographic and timeline  
8 information described herein may either inculcate or exculpate the computer user. Last,  
9 information stored within a computer may provide relevant insight into the computer  
10 user's state of mind as it relates to the offense under investigation. For example,  
11 information within the computer may indicate the owner's motive and intent to commit a  
12 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
13 (e.g., running a "wiping" program to destroy evidence on the computer or password  
14 protecting/encrypting such evidence in an effort to conceal it from law enforcement).  
15 A person with appropriate familiarity with how an electronic device works may, after  
16 examining this forensic evidence in its proper context, be able to draw conclusions about  
17 how electronic devices were used, the purpose of their use, who used them, and when.

18 c. A person with appropriate familiarity with how an electronic device  
19 works may, after examining this forensic evidence in its proper context, be able to draw  
20 conclusions about how electronic devices were used, the purpose of their use, who used  
21 them, and when.

22 d. The process of identifying the exact electronically stored  
23 information on a storage medium that are necessary to draw an accurate conclusion is a  
24 dynamic process. Electronic evidence is not always data that can be merely reviewed by  
25 a review team and passed along to investigators. Whether data stored on a computer is  
26

27  
28 internet browser was used to log into a social media account in the name of John Doe, an  
investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 evidence may depend on other information stored on the computer and the application of  
2 knowledge about how a computer behaves. Therefore, contextual information necessary  
3 to understand other evidence also falls within the scope of the warrant.

4 e. Further, in finding evidence of how a device was used, the purpose  
5 of its use, who used it, and when, sometimes it is necessary to establish that a particular  
6 thing is not present on a storage medium.

7 27. *Nature of examination.* Based on the foregoing, and consistent with Rule  
8 41(e)(2)(B), the warrant I am applying for would permit the examination of the  
9 SUBJECT PHONES consistent with the warrant. The examination may require  
10 authorities to employ techniques, including but not limited to computer-assisted scans of  
11 the entire medium, that might expose many parts of the device to human inspection in  
12 order to determine whether it is evidence described by the warrant.

13 28. *Manner of execution.* Because this warrant seeks only permission to  
14 examine a device already in law enforcement's possession, the execution of this warrant  
15 does not involve the physical intrusion onto a premises. Consequently, I submit there is  
16 reasonable cause for the Court to authorize execution of the warrant at any time in the  
17 day or night.

#### 18 SEARCH TECHNIQUES

19 29. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
20 Rules of Criminal Procedure, the warrant I am applying for will permit imaging or  
21 otherwise copying all data contained on the SUBJECT PHONES, and will specifically  
22 authorize a review of the media or information consistent with the warrant.

23 30. In accordance with the information in this affidavit, law enforcement  
24 personnel will execute the search of the SUBJECT PHONES pursuant to this warrant as  
25 follows:

#### 26 a. **Securing the Data**

27  
28

1 i. In order to examine the ESI in a forensically sound manner,  
2 law enforcement personnel with appropriate expertise will attempt to produce a complete  
3 forensic image, if possible and appropriate, of the SUBJECT PHONES.<sup>2</sup>

4 ii. Law enforcement will only create an image of data physically  
5 present on or within the SUBJECT PHONES. Creating an image of the SUBJECT  
6 PHONES will not result in access to any data physically located elsewhere. However,  
7 SUBJECT PHONES that have previously connected to devices at other locations may  
8 contain data from those other locations.

9 **b. Searching the Forensic Images**

10 i. Searching the forensic images for the items described in  
11 Attachment B may require a range of data analysis techniques. In some cases, it is  
12 possible for agents and analysts to conduct carefully targeted searches that can locate  
13 evidence without requiring a time-consuming manual search through unrelated materials  
14 that may be commingled with criminal evidence. In other cases, however, such  
15 techniques may not yield the evidence described in the warrant, and law enforcement  
16 may need to conduct more extensive searches to locate evidence that falls within the  
17 scope of the warrant. The search techniques that will be used will be only those  
18 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
19 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
20 this affidavit.  
21  
22

---

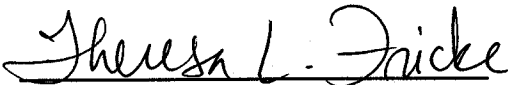
23 <sup>2</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of  
24 digital devices or other electronic storage media is to ensure the integrity of the evidence and to  
25 follow proper, forensically sound, scientific procedures. When the investigative agent is a  
26 trained computer forensic examiner, it is not always necessary to separate these duties.  
27 Computer forensic examiners often work closely with investigative personnel to assist  
28 investigators in their search for digital evidence. Computer forensic examiners are needed  
because they generally have technological expertise that investigative agents do not possess.  
Computer forensic examiners, however, often lack the factual and investigative expertise that an  
investigative agent may possess on any given case. Therefore, it is often important that  
computer forensic examiners and investigative personnel work closely together.

**CONCLUSION**

31. Based on the foregoing, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT PHONES, described in Attachment A to seek the items described in Attachment B.

  
BENJAMIN LONG  
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 3<sup>rd</sup> day of September, 2019.

  
HON. THERESA L. FRICKE  
United States Magistrate Judge



**ATTACHMENT A**

The property to be searched is a Samsung Galaxy J7 Prime, Model Number SM-G610M/DS, Serial Number R58J92RGDSW and an iPhone 7, Model A1661, IMEI 355840088773379 (collectively, the "SUBJECT PHONES"). The SUBJECT PHONES are located at 400 E. Mill Plain Boulevard in Vancouver, Washington. This warrant authorizes the forensic examination of the SUBJECT PHONES for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the SUBJECT PHONES, described in Attachment A, that relate to violations of Title 18, United States Code, Section 2113(b) (Bank Theft), involving PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, and JOSSHOA PEREZ RIVAS, and their co-conspirators, since 2017,<sup>3</sup> including:

- a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, or missed calls;
- c. Stored contact information;
- d. Photographs related to jackpotting or financial accounts and assets held by PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, and JOSSHOA PEREZ RIVAS, or others involved in these activities, or photographs that may show the user of the phone and/or co-conspirators, including any embedded GPS data associated with these photographs;
- e. Stored text messages or other electronic communications related to Jackpotting including Apple iMessages, Blackberry Messenger messages, WhatsApp messages or other similar messaging services where the data is stored on the telephone; and
- f. Information related to financial transactions or accounts, representing the proceeds of jackpotting attacks.

2. Evidence of user attribution showing who used or owned the SUBJECT PHONES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

---

<sup>3</sup> The Washington jackpotting events occurred in 2017.  
ATTACHMENT B – 1  
USAO#2017R01112

1           3.     This warrant authorizes a review of electronic storage media and  
2 electronically stored information seized or copied pursuant to this warrant in order to  
3 locate evidence, fruits, and instrumentalities described in this warrant. The review of this  
4 electronic data may be conducted by any government personnel assisting in the  
5 investigation, who may include, in addition to law enforcement officers and agents,  
6 attorneys for the government, attorney support staff, and technical experts. Pursuant to  
7 this warrant, the FBI may deliver a complete copy of the seized or copied electronic data  
8 to the custody and control of attorneys for the government and their support staff for their  
9 independent review.